GIS-WG draft
Category: Informational
Document: LDAPIETF.doc

Michael Helm
ESnet
February 15, 2001

IETF Directory Report

Status

This document presents a report on recent IETF directory activities and is for informational purposes only.

Abstract

A report on recent IETF activities pertaining to or involving directory. A discussion of areas which bear close attention and involvement by our community follows.

Table of Contents

Introduction

GIS relies exclusively at this time on LDAP. LDAP and X.500 are still evolving in their respective standards organizations. This report will attempt to summarize the current status of relevant working groups in IETF. The events of the last IETF meeting, on-going e-mail discussions, and likely topics of the upcoming IETF meeting of these groups will be summarized.

There are other information and management-related protocols at IETF that the GISWG should probably track, but limitations of time and expertise exclude them from this report.

There are other standards organizations that deal with directories or directory implementations in some way, such as the ITU, the DMTF, and others. The activities of these organizations may be covered by other reports. However, the IETF is the most influential standards body for directory at this time.

Meetings

49th IETF – San Diego, CA, US Dec 2000

50th IETF – Minneapolis MN, US Mar 2001

51st IETF – London, England, UK Aug 2001

See http://www.ietf.org/ for background information.

The Internet Engineering Task Force (IETF) meets three times a year. The cycle for the last several years is two meetings in the US, one non-US. The most recent meetings are listed above.

The IETF now consists of an enormous number of subcommittees, called working groups. Each working group is chartered to develop standards for a specific topical area; the topics have ranged quite far “up the stack” from IP. There are many groups working on topics of interest to GIS. This report focuses on the Directory groups (LDAP), and touches lightly on PKIX. There are other groups that merit attention from GIS: SNMP, DNSOPS, IMPP (instant messaging) among others.

IETF Groups

A pointer to the group’s URL is given, followed by an appraisal of its charter. The charter is then quoted in part. The charter’s milestone section contains only upcoming milestones. The list of documents which follows shows drafts currently under discussion, and RFC’s, which constitute the working group’s completed product.

Following this background material is a summary of the meetings at the 49th IETF, from notes and from the chairperson’s published minutes if any. Each group’s section will conclude with a summary of recent e-mail and agenda for the 50th IETF (if available at time of publication).

LDAPEXT

The Group

http://www.ietf.org/html.charters/ldapext-charter.html

This group is one of the “successor” groups to the original LDAPv3 group. Its purpose was to manage some standards work that was too complex or too immature in development at the time the LDAPv3 drafts were completed and would have slowed the approval of LDAP as a standard. Ironically, LDAPv3 has been blocked from Draft Standard status by a security issue (see LDAPv3*bis*).

There are quite a large number of drafts outstanding. Among the more interesting ones for GIS: Persistent Search, SASL Authentication, Server-Side Sorting, and service location.

Many drafts have advanced to RFC status but a couple of these RFC’s are either informational or are dead ends. Some drafts have been on the table a long time and have waxed and waned in urgency. A few have dropped off the list and subsequently re-instated due to long periods of inactivity.

Description of Working Group:

[This charter is too long (and too out of date) to repeat here.

Goals and Milestones:

(older entries removed)

Mar 00	Submit ID on CLDAP to IESG for consideration as a Proposed Standard
Mar 00	Conclude group or update WG Charter

Internet-Drafts:

The Java LDAP Application Program Interface (242568 bytes)
LDAP Extensions for Scrolling View Browsing of Search Results (26038 bytes)
Persistent Search: A Simple LDAP Change Notification Mechanism (18998 bytes)
The C LDAP Application Program Interface (183118 bytes)
Access Control Model for LDAP (84387 bytes)
X.509 Authentication SASL Mechanism (20431 bytes)
LDAP Control for a Duplicate Entry Representation of Search Results (18268 bytes)
Returning Matched Values with LDAPv3 (19400 bytes)
A Taxonomoy of Methods for LDAP Clients Finding Servers (10785 bytes)
Discovering LDAP Services with DNS (9641 bytes)
Referrals in LDAP Directories (24601 bytes)

Request For Comments:

Lightweight Directory Access Protocol (v3): Extensions for Dynamic Directory Services (RFC 2589) (26855 bytes)
Use of Language Codes in LDAP (RFC 2596) (17413 bytes)
An LDAP Control and Schema for Holding Operation Signatures (RFC 2649) (20470 bytes)
LDAP Control Extension for Simple Paged Results Manipulation (RFC 2696) (12809 bytes)
Access Control Requirements for LDAP (RFC 2820) (18172 bytes)
Authentication Methods for LDAP (RFC 2829) (33471 bytes)
Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security (RFC 2830) (24469 bytes)
LDAP Control Extension for Server Side Sorting of Search Results (RFC 2891) (15833 bytes)

49th IETF

Minutes

http://www2.ietf.org/proceedings/00dec/minutes/LDAPEXT-WG.txt

Intro/Status

Quite a few items completed (see RFC list). Some items active or progressing well (server discovery, JAVA API, C API, cldap, access control models). Some documents need to move to "bis" group, charter needs update; group has been criticized by IETF or area management. The "taxonomy" document is in limbo [probably will move to LDAPv3bis]. The C API draft needs discussion / update but the author couldn't make the meeting (due to Iplanet 5.0 release :^).

DNS SRV (Morgan)

Drop support for ldapv2 and cldap in the document. An interesting discussion about supporting infrastructures that don't have *dc*=…,*dc*=… on the right hand side of a DN. Morgan has received request to drop this restriction but others in the group prefer to keep it. Deferred to mailing list. Most likely the document will limit the namespaces it will attempt to specify and others are on their own.

JAVA LDAP API

A few minor edits reported (see mailing list).

Referrals

Subordinate references soon ready for last call. Cross-references going to draft 01. This will expedite the process.

Duplicate entries

Some discussion of filtering and optimization issues.

LDAP ACI (see also LDAP-ACM below)

No change since 48th IETF (Pittsburgh). Long list of issues worked through from the BOF. New draft by March.

CLDAP

[Connectionless – UDP based] Discussion of LDAPv3 vs v2 issues – different wire formats. Not clear if this is still a viable or particularly interesting topic but work nears conclusion.

Subentry schema

This is shared with the LDUP group. There is some dependency on the schema sub-group as well. Inheritance of ACL's and other policy-like things – how is this implemented? What about multiple policies per sub-entry?
Some need expressed for complex examples of how this standard works (beyond the high-level examples in the current draft). Discussion of X.500 vs LDAP problems – mostly deferred to mailing list.

Group huddle

Goal is to finish up, clearing the current agenda by end of 2001 or earlier. Comment was made that proposals by "lone gunmen" are out; need to have some juice to them (that is, a reasonable chance for multiple implementations) to merit consideration at this time. Also, need to deal with charter review next IETF; submit items. Some documents are moved (subentries above moved to LDUP). A few others moved to LDAPv3bis. What about chaining and proxies? Password work? Discussion about the problems involved in supporting multiple password encryption formats. Finally the group discussed alignment with ITU on directory developments and the upcoming ELSE BOF.

Mailing list activity

ACL model; persistent search; JAVA API; update to authpasswd draft; comments on "cancel extended operation" draft; VLV draft fixes.

50th IETF Agenda

Not available yet

LDAPv3*bis*

The Group

http://www.ietf.org/html.charters/ldapbis-charter.html
This group arose to resolve two issues: (1)Just what is LDAPv3 -- which set of standards describe it and which are extensions? and (2) Remove the IESG security disclaimer and advance LDAPv3 to Draft Standard status. The acceptance of security RFC's xxxx should allow a resolution to (2).
In addition, it was time to fix some "bugs" in the original LDAPv3 standards documents, refining the language, definitions, removing some inconsistencies, and resolving some outstanding problems (old IANA business, X.500 conflicts).
The charter follows.

Description of Working Group:

The LDAPv3 "core" specification is RFC 2251-2256 and 2829-2831. The purpose of this working group is to shepherd these RFCs through the Internet Standard process.
The group will deliver revised LDAPv3 specifications suitable for consideration as a Draft Standard. This work will be based upon RFC 2251-2256,2829-2831.

The group will deliver an applicability statement defining LDAPv3. This work will be based upon draft-hodges-ldapv3-as-00.txt.

Goals and Milestones:

Jun 01	Submit Implementation Report as I-D
Jul 01	Submit LDAP Revised Specification I-Ds and Implementation Report to the IESG for consideration as Draft Standard

Internet-Drafts:

Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names (17528 bytes)
Lightweight Directory Access Protocol (v3) (129435 bytes)
Lightweight Directory Access Protocol (v3):Technical Specification (10770 bytes)
There is also Mark Wahl's taxonomy or glossary draft.

49th IETF

Minutes

The minutes are in the mailing list archives on openldap.org or ftp://ftp.ietf.org/ietf-mail-archive/ldapbis/2001-01.mail. A few extracts from this and from notes follow. The minutes themeselves are a good guide to what is developing in this group.

Introduction

Kurt Zeilinga suggested what was called an engineering approach to dealing with the revision process. Three small documents (replacements for 2253-5) will be finished and advanced to last call ASAP. The others (from the old series as well as some other newer ones) deal with larger issues and will be assigned to one of two "engineering teams". One team will deal with schema, and the other will deal with the protocol and data model. Exactly what documents are needed, what order they will be produced &c will be the responsibility of the teams. This is not "LDAPv4". Changes to be minimized.

Jeff Hodges: Roadmap

This document is on the critical path of everything else and needs to get to proposed ASAP. New draft soon.
For some reason, RFC 2831 ("Using Digest Authentication as a SASL Mechanism", http://www.ietf.org/rfc/rfc2831.txt) is now "owned" by this group. It needs to go to draft standard before everything else can, due to a chain of dependencies. The plan is to try to find a more appropriate owner to expedite this, otherwise will have to deal with it.

Data Model

The strawman changes to RFC 2251-5 and Mark Wahl's taxonomy document were discussed. X.500 vs LDAP: the new documents specify X.500 as a normative reference too, and the difficulty here is figuring out *which* X.500 is the normative reference. How to track the changes in X.500 (admittedly small, but non-zero). An LDAP attribute, X.500/93 and X.500/98 attribute are not all the same thing. Mark Wahl's dictionary attempts to deal with the jargon and undefined assumptions – just what is an "ldap server" anyway? Some discussion took place about tracking changes and formatting the documents so changes and their motivation was clear. What are we going to do about the requirement for a published table of attribute types allowed in DN's? (An IANA registry exists, in a moribund state, but the requirement will resurface once the drafts advance to standard.) How to deal with old RFC's? Deferred to mailing list.

Schema

New draft coming. Similar problems as above with LDAP vs X.500 issues. What about "core" schema vs application or user schema?

Other

Most of the other documents didn't need significant changes at this time.
Mark Wahl suggested adding some protocol examples. An interoperability guide or forum is needed? A summary of changes needs to be kept.
The engineering teams need to report back on document structure. Suggested X.500/93 be chosen as the normative standard as the documents are out of copyright & thus can be reprinted easily.

Mailing List Activity

Attribute values; aliases; Extensible match filters; binary encodings; RFC2252 whitespace; moving some old ldap RFC's to historic status.
Some discussion of the team organization took place, the model is in http://www.openldap.org/lists/ietf-ldapbis/200012/msg00036.html.
The Data Model / Protocol team reached consensus on the following
rough reorganization plan:
  Overview / Data Model
    RFC2251 3.2-3.4
    data model definitions
  Protocol
    RFC2251 (sans 3.2-3.4)
    result code definitions
  Authentication Methods
    RFC2829
Subsequent messages formalize this; expect changes to the milestones. The schema team did not reach a reorganization plan (perhaps none is needed for those RFC's).

50th IETF Agenda

Generic IETF agenda at http://www.openldap.org/lists/ietf-ldapbis/200102/msg00046.html

LDUP

The Group

http://www.ietf.org/html.charters/ldup-charter.html
The other successor group to the original LDAPv3 group. The group has had some very acrimonious meetings in the past. A sharp division exists between a distributed directory contingent, who are willing to give up perfect consistency between replicated directories in order to gain multi-master sources, and a database contingent, who require guaranteed integrity and are uninterested in multi-master sources.

Description of Working Group:

[All but this core paragraph omitted.]
….The WG's approach is to first develop a set of requirements for LDAPv3 directory replication and write an applicability statement defining scenarios on which replication requirements are based. An engineering team was formed consisting of different vendors and the co-chairs in order to harmonize the existing approaches into a single standard approach. All of these have been accomplished during the pre-working group stage. It should be noted, however, that replication using heterogeneous servers is dependent on resolving access control issues, which are the domain of other working groups.

Goals and Milestones:

[Old milestone omitted.]

Mar 00	LDAPv3 Mandatory Replica Management I-D goes to WG Last Call as Proposed Standard.
Mar 00	LDAPv3 Master-Slave Replication Profile I-D goes t WG Last Call as Proposed Standard.
Mar 00	LDAPv3 Multi-Master Replication Profile I-D goes to WG Last Call as Proposed Standard.

Internet-Drafts:

LDUP Update Reconciliation Procedures (69436 bytes)
LDAPv3 Replication Requirements (58887 bytes)
LDAP Replication Architecture (93932 bytes)
LDAP Subentry Schema (21844 bytes)
The LDUP Replication Update Protocol (31961 bytes)

49th IETF

Minutes

The minutes should be in http://www.ietf.org/proceedings/00dec/minutes but it hasn't appeared yet. A draft version appears in the archives of the LDUP mailing list (ftp://ftp.ietf.org/ietf-mail-archive/ldup/2000-12.mail). This is an excellent accompaniment to the drafts. A few extracts and personal notes follow.

Replication Requirements

Much discussion about consistency models. The group seems to have decided to support both model 2 and 3 from the draft document. Models 2 and 3 are loose consistency models that require pre-arrangement with the master. However, the full consistency (ACID) model 1 is not excluded. A long discussion took place on atomicity issues; which seems to conflict with support for multi-master sources. The X.500 specifications for atomicity arose from the single-master nature of X.500 [early X.500?].
The sub-entry draft may introduce more requirements, but the consensus is to freeze the requirements and move on. There was also some discussion of Netscape and interoperability issues to be resolved later. Some semantics of LDAP vs applications discussion.

Replication Architecture

Defines some syntax, ldap extensions, and schema for supporting certain kinds of replications between LDAP servers. A lot of discussion about semantics and the boundary between LDAP and some application, ACL policies as applied to replicating adminstrative areas. Another draft needed for March.

Replication Information Model

Terminology: what constitutes a frame; a group of operations. A group could be interleaved; a frame cannot. Is one subordinate to the other? Not sure. Probably new draft in March.

Subentry Schema (see also LDAPEXT group)

Defer most of this to the draft minutes. The document has been revised extensively over the past few IETF's but still has outstanding areas of difficulty:
Scope – LDAP/LDUP allows many adminstrative areas, but the document is limited to ldapSubEntry containers (which applications can add, for example). Administrative areas are flexible in LDAP, but replication contexts cannot overlap and are bounded by the local DSE (ie cannot span directories). There are difficulties with subentries themselves. Working on visibility and search mechanism. New draft needed.

Discussion of caching and proxy work

… where to put this in IETF?

Mailing List Activity

Charter revision; some additional requirements; Multi vendor directory replication (ACL issues); multi-master replication (as always).

50th IETF Agenda

Not available yet

Schema and ACL subgroups

LDAPEXT-ACM

Description

This is a subgroup working on the Access Control model for LDAP.

Status

This was an interim (read “temporary”) sub-group of ldapext. It seems to have fulfilled its need about a month after the 48th IETF at Pittsburg and returned to ldapext. However, the ACL Model draft was unchanged through the 49th IETF. The Mailing list can be found at http://www.openldap.org/lists/ietf-ldapext-acm/.

ELSE

Description

Evolving ***L***DAP ***S***chema ***E***ntries. This is a subgroup working on schema support.

Status

A BOF was held and a complex table of work areas was produced. The mailing list can be found at http://www.openldap.org/lists/ietf-ldapext-acm/.

Work Areas

http://www.openldap.org/lists/ietf-else/200012/msg00002.html
I was unable to attend this BOF, so I am not sure I can summarize. Instead I will reproduce the table from this message by Tim Harm:

Votes were taken by a show of hands to establish everyone's relative importance of the item. Categories for importance were: Can't live without (CL), Nice to have (Ni), No interest (No), harmful (i.e. contrary to some other working group or effort)

All items that were listed as "Can't live without" or "Nice to have" were then discussed to see who could possibly author a draft on the topic. People who accepted the work are listed in the right hand column of the table.

Description	CL	Ni	No	Harm	Responsible for ID
procedures for merging and updating schema, including a discussion on removing existing schema and understanding when schema elements can be deleted	14	0	0	0	Tim Hahn Ludvic Poitou Mark Hinkley
determine the allowable changes to existing schema elements, define "do no harm" operations, include a	8	4	0	0	Mark Hinkley Tim Hahn to get Bob Moore's

discussion of implications for existing data					document
define extensions to attribute type and object class ABNF to allow for specification of "unique" and "referential integrity"	7	5	0	0	Jim Sermersheim Ludvic Poitou Roger Harrison
define procedures for partitioning, i.e. show how different schemas can be applied to different areas of the DIT	6	7	0	0	Tim Hahn Mark Meredith
updating and removing existing schemas	4	7	0	0	to be handled in the first item above
define a way for ensuring unique attribute type and object class names (not just OIDs)	4	5	0	0	Mortezza Ansari Bob Joslin
discovery of attribute type options that are allowable in a server (was an oversight in LDAPv3 RFCs)	3	10	0	0	Jim Sermersheim Mark Wahl
grouping of LDAP schema pieces, packages of schema, listing dependencies between schema packages, versioning schema packages	0	13	1	0	no one assigned as there exists an Informational RFC 2927 to describe one approach
define how to describe schema as "first class objects" instead of "structured types".	0	8	1	0	Roger Harrison Brian Jarvis
define additional attributes for subschemasubentry. Attributes such as ditContentRules are ill-defined in the current RFCs. This work would clarify their definition and usage	0	7	0	0	Steven Legg
guide LDUP WG on how to replicate schema	0	0	0	17	

Target is March 1, 2001 for draft submissions. This will allow review at next IETF meeting in Minneapolis.

It's not clear if this group remains an independent subgroup or is folding back into the ldapext group.

Mailing List Activity

Some discussion of binary encodings.

50th IETF Agenda

Not available yet

PKIX

The Group

http://www.ietf.org/html.charters/pkix-charter.html
As this group is developing the core standards for an X.509 PKI for the Internet, it is intrinsically linked to Directory. The group is working on schema definitions and "profiles" for the use of LDAP as a certificate and Certificate Revocation List (CRL) storage mechanism. The group is also attempting to produce a certificate validation protocol standard. This will likely result in another distributed Directory application.

Description of Working Group:

[omitted]

Goals and Milestones:

Mar 00 Complete work on attribute certificate profile

Internet-Drafts:

Internet X.509 Public Key Infrastructure Time Stamp Protocols (TSP) (54515 bytes)
Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (108658 bytes)
Internet X.509 Public Key Infrastructure (135330 bytes)
An Internet Attribute Certificate Profile for Authorization (91070 bytes)
Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv3 (13827 bytes)
Simple Certificate Validation Protocol (SCVP) (50558 bytes)
Limited AttributeCertificate Acquisition Protocol (29006 bytes)
Internet X.509 Public Key Certificate Infrastructure and CRL Profile (266861 bytes)
Internet X.509 Public Key Infrastructure Technical Requirements for a non-Repudiation Service (21505 bytes)
Internet X.509 Public Key Infrastructure Qualified Certificates Profile (67842 bytes)
Internet X.509 Public Key Infrastructure Certificate Management Protocols (192046 bytes)
Internet X.509 Public Key Infrastructure Permanent Identifier (17752 bytes)
Transport Protocols for CMP (22549 bytes)
Internet X.509 Public Key Infrastructure Additional LDAP Schema for PKIs and PMIs (39626 bytes)
Internet X.509 Public Key Infrastructure Repository Locator Service (7288 bytes)
Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile (52952 bytes)
Delegated Path Validation (8211 bytes)
Online Certificate Status Protocol, version 2 (44168 bytes)
Delegated Path Discovery with OCSP (8618 bytes)
Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF) (49895 bytes)
The PKIX UserGroupName GeneralName Type (22781 bytes)

Request For Comments:

Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 2459) (278438 bytes)
Internet X.509 Public Key Infrastructure Certificate Management Protocols (RFC 2510) (158178 bytes)
Internet X.509 Certificate Request Message Format (RFC 2511) (48278 bytes)
Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527) (91860 bytes)

Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates (RFC 2528) (18273 bytes)
Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2 (RFC 2559) (22894 bytes)
Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP (RFC 2585) (14813 bytes)
Internet X.509 Public Key Infrastructure LDAPv2 Schema (RFC 2587) (15096 bytes)
X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC 2560) (43243 bytes)
Certificate Management Messages over CMS (RFC 2797) (103357 bytes)
Diffie-Hellman Proof-of-Possession Algorithms (RFC 2875) (45231 bytes)

49th IETF

Minutes

Minutes currently at http://www2.ietf.org/proceedings/00dec/minutes/Incoming/PKIX.txt

Issues relevant to Information Services

LDAP Schema and Protocol

Cross-certification

Certificate & CRL profiles

name constraints

Certificate validation

Another Directory infrastructure

Repository Location

Extracts from PKIX minutes and session notes

Operational Protocols, LDAPv3 - David Chadwick (Univ. of Salford)

This document is the LDAPv3 analog of RFC 2559. This document describes the features of LDAPv3 that are essential, or not required, or are optional for servers to support a PKI based on X.509. David reviewed the mandatory, recommended and not recommended, aspects of the profile.
There was insufficient time for discussion of LDAP schema (see mailing list).

Attribute Certificate Profile

There is a potential security problem when 2 CA's have the same distinguished name. This problem is inherited from the X.509 spec. One CA could issue a certificate with the same serial number and issuer id that properly belongs to the other CA. Probably some correction needs to be made to X.509 for this but until that time the draft will add a paragraph describing this problem.

Repository Location

Repository Locator Service - Phil Hallem-Baker (VeriSign). This document leverages DNS and DNS SRV records to enable Certificate using systems to locate PKI repositories based on a domain name, identify the protocols that can be used to access the repository, and obtain addresses for the servers that host the repository service. The current plan is to progress this as an experimental track RFC.
There was also discussion of an experimental PKI based on XML. May not continue in IETF?

CRL profile

The document is ready for last call, except for a disagreement between PKIX and X.509 published standards about name constraints. PKIX requires the subject field of a CA certificate contain a non-null DN. This issue will be followed up with the ISO group responsible for X.509 in January.

Certficate Validation

There are two alternatives to CRL's under consideration in PKIX, SCVP and OCSP. Most of the time was spent on OCSP issues. PKIX chair is going to attempt to negotiate a settlement (hopefully a merger) of the two proposed protocols. See mailing list.
The issues in OCSP are quite interesting but somewhat complex to summarize. There is a movement to add considerable functionality to the original OCSP, including Delegated Path Discovery (DPD) and Delegated Path Validation (DPV). DPD encompasses techniques for finding the certificates in a certificate chain. DPV encompasses techniques for determining the validity of the certificates on the chain. Michael Myers from VeriSign led a discussion of drafts covering these techniques and the the OCSPv2 draft.

Mailing List Activity

Discussion of LDAP schema needs. Resolution of X.509 problems; Certificate to directory mapping. OCSPv2 issues. This and the related DPV/DPD topics were discussed extensively. These are being split from each other (ie providing DPV and / or DPD doesn't require OCSP and vice-versa!)

50th IETF Agenda

Not available yet

SACRED

The Group

http://www.ietf.org/html.charters/sacred-charter.html
Security credentials (specifically, private keys) are extremely clumsy for humans to handle. They are typically long streams of random bits, unmemorizable but indispensable. This group is developing standards to support two protocols to support portable and easily managed credentials: one involving a credential repository, and another involving peer-to-peer transfer.

Description of Working Group:

There are at least two possible solutions for providing credential portability. The first involves the use of a "credential server". Credentials are uploaded to the server by one device (e.g., a desktop computer); they can be stored there and downloaded when needed by the same or adifferent device (e.g., a mobile phone, PDA, or laptop computer).

A second solution involves the "direct" transfer of credentials from one device to another (e.g., from a mobile phone to a PDA). Although theremay be servers involved in the transfer, in security terms the transfer is direct - that is, there is no "credential server" that takes an active part in securing the exchanges.

Goals and Milestones:

Mar 01 Requirements document to Informational RFC
Mar 01 Frameworks document to Informational RFC
Mar 01 Frameworks document to Informational RFC. Submit second draft of Protocol document
Jun 01 Protocol document to Proposed Standard
Mar 00 Complete work on attribute certificate profile
Securely Available Credentials - Requirements (35574 bytes)
Securely Available Credentials - Framework (31431 bytes)

SACRED Scenarios (19271 bytes)

49th IETF

Draft minutes available from mailing list (ftp://ftp.ietf.org/ietf-mail-archive/sacred/)

Requirements draft:

The credential server is emerging as the most interesting of the standards to develop. The protocol must be capable of supporting a variety of credential formats, and support integrity, privacy, and authentication of some kinds. An interesting discussion about partial authentication techniques between Radia Perlman, Eric Rescorla, and others enused (see the minutes). This came up again in the discussion about authentication methods.

Framework document

Discussion of authentication methods, protocol requirements, how to acquire the trusted root certificates.

Authentication techniques

See minutes for Perlman's paper– outside directory and SACRED scope anyway, but very interesting, discussion of a method for password –based authentication versus other protocols such as SRP.

Mailing List Activity

Credential downloads; patents;

50th IETF Agenda

Not available yet

50th IETF and Out

It appears that the LDUP and PKIX groups will provide some controversial material. The LDAPv3bis group will make good progress towards completing the LDAPv3 specification re-write. It's not clear what LDAPEXT will produce, but several "search" authors have been active on the mailing list. Expect discussion of JAVA API. What's new in schema evolution isn't clear.

Grid Information Services and IETF

IETF groups

The IETF groups responsible for LDAP seem to be in a consolidation phase. LDAPv3bis, the group pulling together and revising the LDAPv3 specifications, is the most important representative of this movement. In order to support widespread adoption of LDAP as a directory standard by other protocols, it must be clear to vendors and developers of LDAP-enabled software precisely what is required.
LDAPv3bis for the most part is not of great concern to GISWG, in so far as GIS accepts the protocol standard as given. Revisions of current RFCs related to LDAP authentication (SASL, TLS) as part of this group should be closely monitored.
It may be prudent to introduce the Globus structural class types to the IETF in the form of an RFC. It is not clear whether the moribund IANA registry for these things will have to be supported (hope not). It is also difficult to support X.509 certificates with unconventional component types (not impossible, but sometimes causes UI problems).
The LDAP extensions group bears watching over the next few IETFs. This is the appropriate format for bringing up new extensions (new syntaxes, schema extensions, control definitions &c) but it is clear that this is not a good time to bring new ideas forward. What is going to happen to schema evolution? There

are currently a large number of “work items” or prospective drafts as shown above in ELSE’s Work Areas. In particular the need for a highly-distributed and multi-platform GIS needs support for distributing, updating, and understanding the schemas in place on directory servers. Perhaps we can either contribute to this specification or investigate implementation issues. More on this after the March IETF.

We are ignoring the currently-experimental partnering of DNS and LDAP DN’s through DC naming (RFC 2247 and the draft “Discovering LDAP Services with DNS”. In particular we are doing precisely what this group chose

Support for directory replication, to support reliability and robustness of a large scale GIS, is an area that is ripe for work. GISWG should be developing interoperability standards and and reliability expectations. There is already enough “history”. However, the LDUP movement may be a place where some of these ideas can be expressed. If we can sample the development as well as influence the standard, we may reduce our problems in the long run. On the other hand this group has had considerable difficulty converging on standards acceptable to the group as a whole.

The security-related groups are only partially in scope, but represent areas of considerable interest to GISWG. PKI’s will require extensive directory support. A verification service like OCSP represents another possible directory implementation. A credential service developed out of SACRED represents not only another directory implementation, but a reliable and trusted (secure) directory, something we are not yet prepared to implement.

Are there problems that need to be brought to the IETF groups?

GIS versus LDAP

1. Danger of falling into proprietary implementation
2. dc component naming problems
3. schema management
4. schema evolution
5. replication protocol
6. replication of ACL’s, schema, and subentry (control area) info
7. dynamic directory
8. Security: Specification of LDAP protocol in PKIX as a model

The PKIX group publishes several documents that describe the relationship with and the requirements that PKIX has for LDAP. One document describes the various protocol elements and whether an LDAP implementation or PKIX must, may, or should support it. PKIX does likewise in some cases for other protocols (ftp, http). This clarifies the relationship between PKIX and these protocols. Perhaps we should do likewise.

Some of the larger IETF groups, such as the DNS extensions group and PKIX, produce “roadmap” documents that describe how the documents work together, the expected evolution, and the basis for the work. The PKIX roadmap is indispensable for that group: “Internet X.509 Public Key Infrastructure”, but known currently as draft-ietf-pkix-roadmap-06.txt. We should consider doing likewise; we are headed in that direction on the website.

We are in some danger of creating a “proprietary” directory infrastructure. It would be one that looked a lot like LDAP up close, but diverged from it greatly in the aggregate and in the philosophy. Perhaps this is a good thing, but this kind of divergence should be undertaken deliberately. Clarifying the relationship between GIS and LDAP would be worthwhile, in every respect.

There is a moribund dynamic directory RFC from LDAPEXT (RFC 2589). This has some limitations (among other things, it’s dynamic at the entry level, not the attribute level). Vendors are not currently interested in implementing this. Nevertheless, it already exists as a standards track document. Perhaps we should look at this more closely, and consider how we could encourage an implementation effort.

Conclusion

The IETF directory groups were introduced: their charters, their immediate milestones, and their current document product was reviewed, with extracts from those documents, and notes from recent IETF sessions. Some review of upcoming sessions was made. A brief discussion of areas of common interest was made – are there areas we should be working in common, items and extensions we should be adopting as our own standards? There are also some coordinating discussions that need to be done, probably to end in documents that revisit the original MDS specifications and the relationship between directories.

A similar but shorter IETF report may appear in future Gridforums.